UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,227	09/27/2001	Jeffrey Scott Bardsley	RSW920010166US1	5924

7590 10/21/2005

Jack Friedman
SCHMEISER OLSEN and WATTS
3 Lear Jet Lane
Suite 201
Lathan, NY 12110

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/966,227	Applicant(s) BARDSLEY ET AL.	
	Examiner Matthew T. Henning	Art Unit 2131	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 20 June 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: *None*.
   Claim(s) objected to: *None*.
   Claim(s) rejected: *1-18*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Continuation of 3. NOTE: Claim 5 recites the limitation of monitoring, by the IDS...impede operation of the protected device..

Continuation of 11. does NOT place the application in condition for allowance because: In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., monitoring, by the intrusion detection system, ...impede operation of the protected device) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, these new limitations, which have not been entered, were presented in the claims after final rejection and therefore would require further consideration. Therefore, the argument is not persuasive.

The examiner notes that the following arguments were presented in the communication filed 2/1/2005 and were considered and counter arguments were presented in the final rejection dated 4/28/2005. However, the applicant's have not responded to the counter arguments that were presented. Accordingly, the counter arguments have been presented again below.

In response to applicant's argument with regards to claims 1-2, 5, and 8-10, that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Freidman provides a system which squelches alert generation (See Freidman Col. 13), and Shanklin teaches an intrusion detection system that generates alerts and sends them to a system manager (See Shanklin Col. 3 Lines 13-16). Chari teaches that by sending and receiving all alerts, network traffic increases and available bandwidth decreases. Also, the volume of alerts received by the network administrator can overwhelm the administrator (See Chari Col. 2 Lines 55-65). Chari provides motivation to squelch the alerts of Shanklin and therefore the motivation to combine the alert squelcher of Freidman and the alerting system of Shanklin. Therefore, a prima facie case of obviousness was made because the ordinary person would have been motivated to "ensure that the system manager of [Shanklin] was not overwhelmed by alerts" and the ordinary person skilled in the art would have been motivated to ensure "that the network [of Shanklin] was not bottlenecked with alerts". Therefore, the examiner does not find the applicants' argument persuasive.

Regarding applicants' argument that the combination of Freivald and Shanklin did not disclose a log, the examiner does not find the argument persuasive. Freivald disclosed storing the last modified header (See Freivald Col. 7 Lines 39-41) and although this is not specifically called a log, it is in fact a log. Furthermore, Shanklin disclosed logging the alerts generated by the IDS (See Shanklin Col. 1 Lines 33-38). Therefore, the combination of Freivald and Shanklin did in fact disclose a log, and the examiner does not find the argument persuasive.

Accordingly, the rejections of claims 1-18 have been maintained..